REMARKS

Claims 1-6 and 9 are pending in the application and stand rejected.

Rejection under 35 U.S.C §103

Claims 1 and 9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich in view of U.S. Pat. No. 5,898,784 to Kirby et al. In his first Response, Applicant explained that Redlich does not in fact disclose all claimed limitations. In the second Action, the Examiner answered that Redlich does in fact teach "each PDU having a message-type field by which the security entity in the intermediate system can determine whether a PDU it receives encapsulates a PDU to be extracted and sent on" because the Examiner reads Redlich's message-type field as being the PDU's port number that is used to determine where a PDU should be routed, and insisted that Redlich contemplates multiple tunnels being available. In the last filed Response, Applicant amended the claims to set out their scope with greater clarity, and again endeavored to explain that Redlich only sets up one security session, with the tunnel server, and does not set up a security session with the target system, as this is unnecessary because the tunnel server itself exists in a trusted environment. Although the tunnels between the access router and outside router are secure tunnels, they are not set up by the guest station but by the access router to ensure that guest packets cannot leak out behind the host network's firewall.

In the present Action, the Examiner does not reply to Applicant's arguments but rather merely dismisses them as moot in view of new grounds of rejection. This time, the Examiner does acknowledge that Redlich fails to teach each first PDU having a message-type field for indicating to the security entity in the intermediate system whether a said first PDU it receives encapsulates a second PDU that is to be extracted and sent on. However, the Examiner asserts that Kirby teaches precisely this feature at col. 5 ll. 55-63, which recites:

> The tunnel may also indicate where the packet is to be sent. Primary firewall computers 16, 18 store information about the internal path of each tunnel in a tunnel database. When computer 146 receives a packet whose policy id indicates that the packet came through a tunnel that ends at computer 146, e.g., tunnel 142,

computer 146 decapsulates and decrypts the packet and sends the decrypted packet over internal network 154 to the proper destination computer in accordance with the decrypted destination address.

Applicant respectfully submits that the Examiner has failed to appreciate a key difference between the cited art and the presently claimed invention, namely that in Kirby, communication of packets occurs over multiple tunnels, each belonging to a different security session, whereas the present claims are directed to a method and system wherein a single tunnel hosts nested security sessions. Furthermore, just like Redlich, Kirby fails to disclose *nested* security sessions.

Kirby is essentially concerned with firewall computers that operate to encrypt and encapsulate data packets within other packets that are exchanged with other firewall computers, and is particularly concerned with the establishment of multiple tunnels between such firewall computers for the secure transmission of these packets between the remote internal networks that are protected by these firewall computers. Figure 8 of Kirby provides a good overview of his general arrangement, wherein two firewall computers 146 and 148 are connected to a respective internal network, and further communicate with one another across external network 152. The internal network associated with firewall computer 146 is shown to further include an internal firewall computer 158. Kirby makes abundantly clear that multiple tunnels are set up between the firewall computers 146 and 148 (please see, e.g., Kirby at col. 5 l. 37 through col. 6 l. 24). Furthermore, it is important to note that such tunnels may either terminate at a firewall computers (for instance, tunnel 142 which terminates at firewall computer 146) or may simply pass through a firewall computer (such as tunnel 140 which terminates at internal firewall computer 158).

Each encrypted packet that is transmitted can be decrypted only by the particular computer to which the packet is addressed, as set forth in the policy id field 113 that is found in the header of each packet. Thus, the point of termination of each tunnel set up between two firewall computers is not arbitrary, and each tunnel must terminate at a specific computer. The firewall computers determine what tunnel each received packet belongs to by inspecting the policy id field of each packet, and take appropriate subsequent action; for instance, firewall

computer 146 determines whether received packets belong to tunnel 142, and unpacks such packets to extract and decrypt their encapsulated packets to then send on to their final destination computer, or whether received packets belong to tunnel 140, which are then sent on to internal firewall computer 158 where they are unpacked and the encapsulated packets decrypted and sent on to their final destination computer.

It is important to understand that the present claims are directed to a method and system wherein a *single tunnel* is set up from the subject system to the intermediate system. Thus, the subject system sets up a *first security session* with the intermediate system and sends first PDUs to the intermediate system via this first security session. Some of these first PDUs encapsulate second PDUs that are intended to be sent on to another system, and these second PDUs thereby represent a *second security session* that is set up between the subject system and this other system. Thus, in the present system, all PDUs received by the intermediate system (the first PDUs) are unpacked by the intermediate system and, if any of them contain second PDUs, these second PDUs are sent on to their final destination. Those first PDUs that do not contain second PDUs for further transmission are treated as containing data that is intended for the intermediate system. Thus, in the present system, there are two types of first PDUs (those that encapsulate second PDUs and those that do not) but all first PDUs belong to the first security session, and the intermediate system uses the message-type field of the first PDUs to distinguish between the two types of first PDUs that are found in the first security session but regardless, unpacks all first PDUs.

This is in direct contrast with Kirby, where the policy id field is used to differentiate between different tunnels; by definition, different tunnels belong to different security sessions, and thus each firewall computer of Kirby receives and distinguishes between packets belonging to different security sessions, not to the same security session. Also significantly, each firewall computer of Kirby unpacks only those packets that authorize the firewall computer to unpack them and sends other packets on to other computers on its respective internal network without unpacking them, whereas in the present system all PDUs received by the intermediate system are unpacked at the intermediate system.

Thus, even if a skilled person were motivated to attempt to modify the system of Redlich to utilize the method of Kirby, as alleged by the Examiner, the result would be a system/method wherein communication occurs over multiple tunnels, and packets are unpacked only at their ultimate destination computer. This has been shown to be in direct contrast with Applicant's claimed invention. Furthermore, Applicant does not agree that either Kirby or Redlich contain the requisite teaching that could provide the required motivation for a skilled person to attempt the combination alleged by the Examiner. The Examiner opines that the skilled person would have found it obvious to utilize Kirby's method of forwarding packets with Redlich's system because it offers the advantage of allowing routing of packets to a correct destination in accordance with the virtual tunnel it came from. However, Redlich is concerned with the protection of a network that allows a guest station to connect to it and access the Internet through it. Thus, Redlich discusses solely methods for the host network to manage and control the communication between the guest station and the outside world occurring through the host network and its external access routers. Kirby, on the other hand, is concerned with the operation of a firewall receiving communications from the outside world and deciding how to distribute these communications to the internal network that it is protecting. There is absolutely no need for one practicing the invention of Redlich to be concerned with "routing packets to a correct destination in accordance with the virtual tunnel it came from" because this simply makes no sense within the context of Redlich's arrangement. Redlich and Kirby are concerned with completely disparate aspects of network management and operation, and there is no objective reason for any skilled person practicing one invention to feel motivated to consult the disclosure of the other.

Nonetheless, in an effort to set forth the above differences in the claims in an even clearer and more unambiguous manner, Applicant has further amended independent claims 1 and 9 to specify that the message-type field in each first PDU is for indicating to the security entity in the intermediate system whether a said first PDU it receives encapsulates a said second PDU that is to be extracted and sent on or whether it holds data for use by the intermediate system. Applicant thus submits that, in view of all of the above as well as previously presented arguments and amendments, claims 1 and 9 are in fact novel and patentable over the cited art, and respectfully request the Examiner to reconsider and pass both claims to issue.

Claim 2 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich in view of U.S. Pat. No. 5,898,784 to Kirby et al., claims 3-5 as being unpatentable over Redlich in view of U.S. Pat. No. 6,081,306 to Subramaniam, and claim 6 as being unpatentable over Redlich in view of U.S. Pat. No. 6,574,224 to Brueckheimer.

Claims 2-6 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Applicant submits that claims 2-6 are also allowable.

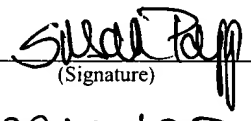
In view of the above, Applicant submits that the application is now in condition for allowance and respectfully urges the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

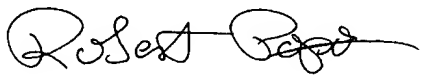
August 3, 2005
(Date of Transmission)

Susan Papp
(Name of Person Transmitting)


(Signature)

08/03/05
(Date)

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com